

Abstract of Reference 3

SECURITY SYSTEM

Publication number: JP2003085661 (A)

Publication date: 2003-03-20

Inventor(s): YAMAUCHI UMEO; YAMAGUCHI KANICHI +

Applicant(s): YAMAUCHI JIMUSHO KK; YAMAGUCHI KANICHI +

Classification:

- international: B60R25/10; E05B49/00; G03B15/00; G08B13/196; G08B21/00; H04N5/225; H04N7/18; H04N101/00; B60R25/10; E05B49/00; G03B15/00; G08B13/194; G08B21/00; H04N5/225; H04N7/18; (IPC1-7): B60R25/10; E05B49/00; G03B15/00; G08B13/196; G08B21/00; H04N101/00; H04N5/225; H04N7/18

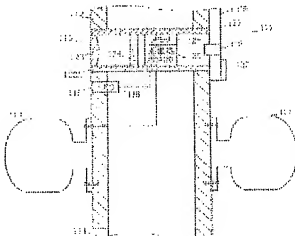
- European:

Application number: JP20010246087 20010814

Priority number(s): JP20010246087 20010814; JP20010180638 20010614; JP20010203062 20010704

Abstract of JP 2003085661 (A)

PROBLEM TO BE SOLVED: To provide a security system capable of effectively preventing unauthorized intrusion of a burglar or the like, a robbery or illegal actions. SOLUTION: A hole 116 for illumination is opened on a door 112. An optical lens 123 and a CCD 124 are arranged inside a hole 115 for image pickup, and when there is a visitor 117, it is detected and the image is picked up. Image data processed in an image processing circuit 126 are recorded in a memory 126 sheet by sheet. The image can be viewed on a liquid crystal display 129 and can be taken out from an image data output terminal to the outside as well. The memory 126 can not be detached since it is housed inside the door 112. By photographing the image, the intrusion can be prevented. For the unauthorized intrusion, there is a high possibility of being able to specify the date and time and a face of an intruder or the like by the image. It is also possible to confirm the image or the like and invite the visitor 117 into a prescribed place.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-85661

(P2003-85661A)

(43) 公開日 平成15年3月20日 (2003.3.20)

(51) Int.Cl. ⁷	識別記号	F I	サーチコード [*] (参考)
G 0 8 B 13/196		G 0 8 B 13/196	2 E 2 5 0
B 6 0 R 25/10	6 2 1	B 6 0 R 25/10	6 2 1 5 C 0 2 2
	6 2 5		6 2 5 5 C 0 6 4
E 0 5 B 49/00		E 0 5 B 49/00	K 5 C 0 8 4
G 0 3 B 15/00		G 0 3 B 15/00	S 5 C 0 8 6

審査請求 未請求 請求項の数30 O L (全 25 頁) 最終頁に続く

(21) 出願番号 特願2001-246087(P2001-246087)

(22) 出願日 平成13年8月14日 (2001.8.14)

(31) 優先権主張番号 特願2001-180638(P2001-180638)

(32) 優先日 平成13年6月14日 (2001.6.14)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願2001-203062(P2001-203062)

(32) 優先日 平成13年7月4日 (2001.7.4)

(33) 優先権主張国 日本 (J P)

(71) 出願人 599172726

有限会社 山内事務所

川崎市麻生区正禅寺1438-288

(71) 出願人 598118927

山口 寛一

東京都新宿区西新宿5-17-11

(72) 発明者 山内 梅雄

神奈川県川崎市麻生区正禅寺2丁目10番7号

(74) 代理人 100083957

弁理士 山内 梅雄

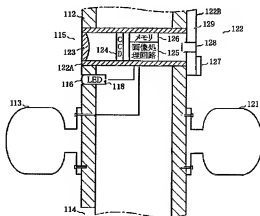
最終頁に続く

(54) 【発明の名称】 セキュリティシステム

(57) 【要約】

【課題】 泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することのできるセキュリティシステムを得ること。

【解決手段】 ドア112には照明用孔116が開けられている。撮像用孔115の内部には光学レンズ123とCCD124が配置されており、来訪者117があるとこれが検知されてその画像が撮られる。画像処理回路126で処理された画像データはメモリ126に1枚ずつ記録される。この画像は液晶ディスプレイ129で見ることでもできるし画像データ出力端子から外部に取り出すこともできる。メモリ126はドア112内部に収容されているので、取り外すことができない。画像を撮影することで侵入を防止することができる。無断侵入に対してはその日時および侵入者の顔を画像で特定できる可能性が高い。画像等を確認して来訪者117を所定の場所に招き入れることも可能である。



【特許請求の範囲】

【請求項1】 扉と、

この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、

この撮像手段を動作させるトリガ手段と、

前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項2】 人の出入りするための扉と、

この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、

この撮像手段を動作させるトリガ手段と、

前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。

【請求項3】 ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、

前記ドアの内側面に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項4】 ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、

前記ドアの内側面に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項5】 交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、

前記ドアの内側面に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項6】 交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、

前記ドアの内側面に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。

【請求項7】 交通機関の所定の部位に穿たれた孔と、その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項8】 交通機関の所定の部位に穿たれた孔と、その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。

【請求項9】 通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、

この撮像手段を動作させるトリガ手段と、

前記壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項10】 通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、

この撮像手段を動作させるトリガ手段と、

前記壁の表面よりも奥側に収容され、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。

【請求項11】 人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、

この容器に穿たれた孔と、

この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とを具備することを特徴とするセキュリティシステム。

【請求項12】 人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、この容器に穿たれた孔と、

この孔を通して外部を撮影する撮像手段と、

この撮像手段を動作させるトリガ手段と、

このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とを具備することを特徴とするセキュリティシステム。

ム。

【請求項13】 前記トリガ手段は人等の物体の接近を検出するセンサであることを特徴とする請求項1～請求項12いずれかに記載のセキュリティシステム。

【請求項14】 前記トリガ手段は外部の物体の動きを検出して撮像手段を動作させることを特徴とする請求項1～請求項12いずれかに記載のセキュリティシステム。

【請求項15】 前記トリガ手段は、予め定めた時間ごとに撮像手段を動作させることを特徴とする請求項1～請求項12いずれかに記載のセキュリティシステム。

【請求項16】 前記撮像手段の近傍に外部の音を収集するマイクロフォンが配置されており、収集された音を撮像データと共に処理することを特徴とする請求項1～請求項12いずれかに記載のセキュリティシステム。

【請求項17】 前記孔はキーホールに似せた撮像のための孔であることを特徴とする請求項3～請求項8、請求項11または請求項12いずれかに記載のセキュリティシステム。

【請求項18】 撮像の時刻情報が撮像データに組み込まれることを特徴とする請求項1～請求項12いずれかに記載のセキュリティシステム。

【請求項19】 前記撮像データ記憶手段は画像を順次1枚ずつ記憶し、予め定められた枚数に到達したときには古い画像から順に上書きして記憶することを特徴とする請求項1、請求項3、請求項5、請求項7、請求項9、請求項11いずれかに記載のセキュリティシステム。

【請求項20】 前記所定の受信先は予め定めた携帯端末等の通信端末であることを特徴とする請求項2、請求項4、請求項6、請求項8、請求項10、請求項12いずれかに記載のセキュリティシステム。

【請求項21】 前記所定の受信先は駐車場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されることを特徴とする請求項2、請求項4、請求項6、請求項8、請求項10、請求項12いずれかに記載のセキュリティシステム。

【請求項22】 人の出入りするための扉と、この扉あるいはその近傍に埋め込まれる扉の前の被写体を撮像する撮像手段と、この撮像手段を動作させるトリガ手段と、前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、この撮像データ発信手段の発信に基づく前記受信先との通信中に受信先から開錠を指示する信号が送られてきたとき前記扉を開錠する開錠手段とを具備することを特徴とするセキュリティシステム。

【請求項23】 人の出入りするための扉と、

この扉あるいはその近傍に埋め込まれる扉の前の被写体を撮像する撮像手段と、

この撮像手段を動作させるトリガ手段と、前記扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、この撮像データ発信手段の発信先によって撮像データを送信しないとき、予め定めた発信先へこれを転送する転送手段と、

この撮像データ発信手段の発信に基づく前記発信先との通信中にその発信先から開錠を指示する信号が送られてきたとき前記扉を開錠する開錠手段とを具備することを特徴とするセキュリティシステム。

【請求項24】 前記孔から前記撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備することを特徴とする請求項3～8いずれかに記載のセキュリティシステム。

【請求項25】 前記孔から前記撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の発信先に送る警報データ送出手段を具備することを特徴とする請求項3～8いずれかに記載のセキュリティシステム。

【請求項26】 前記孔は複数配置されており、前記トリガ手段は、障害検出手段が1つの孔の障害を検出したとき他の孔の内部に配置された前記撮像手段を動作させることを特徴とする請求項24または請求項25記載のセキュリティシステム。

【請求項27】 交通機関の走行のための動力源が始動されたときこれを検出する動力源始動検出手段と、この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関の所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、

この特定通信端末有無判別手段がその特定通信端末が存在しないときその特定通信端末に対して前記交通機関の動力源が始動されたことを無縁で通知する通知手段とを具備することを特徴とするセキュリティシステム。

【請求項28】 交通機関の走行のための動力源を動作させるキーを挿入するキー挿入口と、このキー挿入口にキーが挿入され前記動力源が始動されたときこれを検出する動力源始動検出手段と、この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関のキー所有者の所持する特定通信端末が存在するか否かを通信によって判別する特定通信端末有無判別手段と、この特定通信端末有無判別手段がその特定通信端末が存在しないときその特定通信端末に対して前記

交通機関の動力源が始動されたことを無線で通知する通知手段とを具備することを特徴とするセキュリティシステム。

【請求項29】 前記交通機関の運転席あるいはその近傍を撮像する撮像手段を備え、前記通知手段はこの撮像した画像を送信して前記特定通信端末にこれを送信することを特徴とする請求項27または請求項28記載のセキュリティシステム。

【請求項30】 前記通知手段の通知に基づいて前記特定通信端末から前記交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行う交通機関制御手段を具備することを特徴とする請求項27または請求項28記載のセキュリティシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は盗難、無断侵入を防止したり、所定の場所を出入りする者をチェックあるいは管理するためのセキュリティシステムに係わり、たとえば自動車、バイク、船舶等の交通機関、家屋、金庫、エレベーター、洗面所の入り口、飛行機の搭乗口等の各物あるいは場所を使用することのできるセキュリティシステムに関する。

【0002】

【従来の技術】家屋や車に対する無断侵入や金庫等の保管容器内の物品の盗難を防止する等のために鍵が広く使用されている。また、防犯用のテレビカメラも使用されている。

【0003】

【発明が解決しようとする課題】ところが、通常の鍵は熟練した泥棒の多くが簡単に開けることができる。このため、より複雑な構造をした鍵が考案されているが、時間がかければそのほとんどが開けられてしまう。したがって、現状では玄関ドアに複数の鍵を付けて、泥棒が開けるまでの時間を稼ぐことで泥棒に侵入を敬遠させるといった手法が勧められている。しかしながら、泥棒が一度ドアを開けて侵入したことがあれば、その者の足跡は掴みにくのが通常であり、事件は未解決に終わることも多い。

【0004】また、防犯用のテレビカメラはその位置および撮影範囲が外部から特定されるので、その死角を利用して犯罪が行われることがあえる。また、テレビカメラ自体を事前に撮影不能にすることも場合によって可能である。更にテレビカメラの設置にはある程度の場所が必要であって、小型の自動車や金庫等に配置することができない。また、設備の購入および維持のためのコストがかかり高いという問題もある。

【0005】以上、泥棒を中心に説明したが、テレビカメラは人の管理にも使用されているものの、同様の問題がある。

【0006】そこで本発明の目的は、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することのできるセキュリティシステムを提供することにある。

【0007】

【課題を解決するための手段】請求項1記載の発明では、(イ)扉と、(ロ)この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0008】すなわち請求項1記載の発明では、撮像手段が扉あるいはその近傍に埋め込まれており、扉の前の被写体を撮像するようになっている。撮像データ記憶手段は、扉あるいはその近傍に埋め込まれており、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶するようになっている。撮像手段がデジタルカメラの普及によって小型化かつ高性能化したので、たとえばその構成部品を扉あるいはその近傍に埋め込むことが可能になる。撮像データ記憶手段も、扉あるいはその近傍に埋め込まれるので、自分が撮影されたことに気づいた侵入者等は撮影された画像を消去したり撮像データ記憶手段自体を取り出すことが困難であり、早急に現場を立ち去ることになるので、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。撮像データとして動画を得ることも可能であるが、特に静止面を得る場合には、僅かのメモリ容量で多くの静止面を得ることができる。また振動写真と比べてランニングコストをわずかに抑えることができ、また事件が起きたときには画像データを有効な資料とすることができる。

【0009】請求項2記載の発明では、(イ)人の出入りするための扉と、(ロ)この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の発信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0010】すなわち請求項2記載の発明では、撮像手段が扉あるいはその近傍に埋め込まれており、扉の前の被写体を撮像するようになっている。撮像データ発信手段は、扉あるいはその近傍に埋め込まれており、トリガ手段によって作動した撮像手段から得られる撮像データを所定の発信先に発信するようになっている。撮像手段がデジタルカメラの普及によって小型化かつ高性能化したので、たとえばその構成部品を扉あるいはその近傍に埋め込むことが可能になる。撮像データ発信手段も扉あるいはその近傍に埋め込まれているので、発信を安全に行うことができる。しかも本発明の場合には画像自体は

所定の受信先に送られてしまうので、仮に撮像手段や撮像データ発信手段が持ち去られたとしても、画像の記録は残ることになり、結局、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。撮像データとして動画を得ることも可能であるが、特に静止画を得る場合には、多くの画像を短時間に送信することができる。

【0011】請求項3記載の発明では、(イ)ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、(ロ)ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0012】すなわち請求項3記載の発明では、ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ記憶手段は、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する。このように小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮影することにしたので、ドア自体を加工する必要がない。ドアノブに本発明を適用することで、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。また、台座の表面に凹凸を付けたようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【0013】請求項4記載の発明では、(イ)ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に穿たれた孔と、(ロ)ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0014】すなわち請求項4記載の発明では、ドアの外側部分に突出して取り付けられたドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、事故の発生や友人等の来訪を迅速に知ることができる。更に撮像データを発信することにしたので、ドアノブ側に大量のメモリが不要であり、大量の静

止画だけでなく、動画を撮る時間の制限も緩和される。また、台座の表面に凹凸を付けたようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【0015】請求項5記載の発明では、(イ)交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、(ロ)ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0016】すなわち請求項5記載の発明では、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ記憶手段は、トリガ手段によって作動した撮像手段から得られる撮像データを逐次記憶する。このように小型化された撮像のための装置をドアの把手あるいはこの把手に取り付けられた付属部品の孔から撮影することにしたので、ドア自体を加工する必要がない。ドアの把手あるいはこの把手に取り付けられた付属部品を本発明のものとすることで、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【0017】請求項6記載の発明では、(イ)交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に穿たれた孔と、(ロ)ドアの内部側に配置され、この孔を通して外部を撮影する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0018】すなわち請求項6記載の発明では、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿っている。撮像手段はドアの内部側に配置され、この孔を通して外部を撮影するようになっている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、その交通機関自体が盗難にあった場合も画像データ自体は安全な箇所に保持されることになり、盗難の犯人の特定が容易になる。また、結果的には盗難あるいは不正行為の発生を有効に防止することができる。

【0019】請求項7記載の発明では、(イ)交通機関の所定の部位に穿たれた孔と、(ロ)その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮

像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって動作した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0020】すなわち請求項7記載の発明では、請求項5および請求項6と異なり、ドアの把手あるいはこの把手に取り付けられた付属部品以外の場所でも孔を開けることができ、同様に本発明を適用可能であることを示している。交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容すればよい。これらの部品を必要に応じて交換することで、本発明による盗難防止等の利益を得ることができる。

【0021】請求項8記載の発明では、(イ)交通機関の所定の部位に穿たれた孔と、(ロ)その孔を穿った部分の内部に配置され、この孔を通して外部を撮影する撮像手段と、(ハ)この撮像手段を動作させるトリガ手段と、(ニ)このトリガ手段によって動作した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0022】すなわち請求項8記載の発明では、請求項5および請求項6と異なり、ドアの把手あるいはこの把手に取り付けられた付属部品以外の場所でも孔を開けることができ、同様に本発明を適用可能であることを示している。交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容すればよい。これらの部品を必要に応じて交換することで、本発明による盗難防止等の利益を得ることができる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【0023】請求項9記載の発明では、(イ)通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、(ロ)この撮像手段を動作させるトリガ手段と、(ハ)壁の表面よりも奥側に収容され、このトリガ手段によって動作した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0024】すなわち請求項9記載の発明では、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようにになっている。撮像データ記憶手段は、壁の表面よりも奥側に収容され、このトリガ手段によって動作した撮像手段から得られる撮像データを逐次記憶するようにになっている。壁の表面よりも奥側とは、必ずしも壁の内部とは限らず、たとえばその壁の向こう側の部屋の内部や天井部分であってもよい。要は第三者が撮像データ記憶手段に対してアクセスしにくい場所をいう。本発明でも、撮影された者はなす術がないので、結局、無断侵入や盗難あるいは不正行為の発生を

有効に防止することができることになる。

【0025】請求項10記載の発明では、(イ)通路または部屋の壁に埋め込まれ壁の前の被写体を撮像する撮像手段と、(ロ)この撮像手段を動作させるトリガ手段と、(ハ)壁の表面よりも奥側に収容され、このトリガ手段によって動作した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0026】すなわち請求項10記載の発明では、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようにになっている。撮像データ発信手段は、壁の表面よりも奥側に収容され、このトリガ手段によって動作した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。壁の表面よりも奥側とは、必ずしも壁の内部とは限らず、たとえばその壁の向こう側の部屋の内部や天井部分であってもよい。要は第三者が撮像データ記憶手段に対してアクセスしにくい場所をいう。本発明でも、撮影された者はなす術がないので、結局、無断侵入や盗難あるいは不正行為の発生を有効に防止することができることになる。しかも本発明では撮像データ発信手段を配置しているので、画像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【0027】請求項11記載の発明では、(イ)人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、(ロ)この容器に穿たれた孔と、(ハ)この孔を通して外部を撮影する撮像手段と、(ニ)この撮像手段を動作させるトリガ手段と、(ホ)このトリガ手段によって動作した撮像手段から得られる撮像データを逐次記憶する撮像データ記憶手段とをセキュリティシステムに具備させる。

【0028】すなわち請求項11記載の発明では、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしている。撮像データ記憶手段は、トリガ手段によって動作した撮像手段から得られる撮像データを逐次記憶するようになっている。借家主まいのように扉または通路自体の改造が難しい場合には、このような容器を適所に取り付けることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【0029】請求項12記載の発明では、(イ)人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器と、(ロ)この容器に穿たれた孔と、(ハ)この孔を通して外部を撮影する撮像手段と、(ニ)この撮像手段を動作させるトリガ手段と、(ホ)このトリガ手段によって動作した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段とをセキュリティシステムに具備させる。

【0030】すなわち請求項1記載の発明では、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしている。撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようにしている。したがって、その容器自体が破壊されたり持ち去られるような場合でも、その行為を行った者の画像を取得することができ、結果的にそのような行為自体も防止することができる。

【0031】請求項1記載の発明では、請求項1〜請求項12いずれかに記載のセキュリティシステムで、トリガ手段は人等の物体の接近を検出するセンサであることを特徴としている。

【0032】すなわち請求項1記載の発明では、画像の撮影を開始するトリガ手段は人等の物体の接近を検出するセンサであることを特徴としている。撮影は静止画であれば1枚または所定枚数を間隔を置いて行う。センサが検知している期間に渡って所定間隔で静止画を撮り続けるようなものでもよい。動画であればその期間あるいはタイマによって設定した時間だけ画像を撮り続けることになる。

【0033】請求項1記載の発明では、請求項1〜請求項12いずれかに記載のセキュリティシステムで、トリガ手段は外部の物体の動きを検出して撮像手段を作動させることを特徴としている。

【0034】すなわち請求項1記載の発明では、画像の撮影を開始するトリガ手段は外部の物体の動きを検出して撮像手段を作動させることを特徴としている。撮影は静止画であれば1枚または所定枚数を間隔を置いて行う。センサが検知している期間に渡って所定間隔で静止画を撮り続けるようなものでもよい。動画であればその期間あるいはタイマによって設定した時間だけ画像を撮り続けることになる。動きを検出するので、人の接近等を効果的に検出できる。

【0035】請求項15記載の発明では、請求項1〜請求項12いずれかに記載のセキュリティシステムで、トリガ手段は、予め定めた時間ごとに撮像手段を作動させることを特徴としている。

【0036】すなわち請求項15記載の発明では、画像の撮影を開始するトリガ手段は、たとえば1分置きというように予め定めた時間ごとに撮像手段を作動させる。静止画であれば画像データの1枚あたりの量はそれほど多くないので、半導体のメモリであっても数日分の画像を簡単に記憶させることができる。また、画像データを送信する場合には発信側にメモリ容量の制限がないので、時間間隔を狭くしても問題が生じることは少ない。本発明では、トリガ用に特別のセンサが不要であるので、確実に無断侵入や盗難あるいは不正行為の事実を記録す

ることができる。

【0037】請求項16記載の発明では、請求項1〜請求項12いずれかに記載のセキュリティシステムで、撮像手段の近傍に外部の音を収集するマイクロフォンが配置されており、収集された音を撮像データと共に処理することを特徴としている。

【0038】すなわち請求項16記載の発明では、画像データと共に音のデータも収集することを示している。音の収集だけでなく発声も行えるようにすれば、自宅を留守にしているような場合でも、ドアホンを使用している感覚で携帯電話機等を使用して訪問者等と会話が可能になる。

【0039】請求項17記載の発明では、請求項3〜請求項8、請求項11または請求項12いずれかに記載のセキュリティシステムで、孔はキーホールに似せた撮像のための孔であることを特徴としている。

【0040】すなわち請求項17記載の発明では、撮像のための孔をキーホールに似せたものにすることでカムフラージュして、本人が気付かないうちに撮影が可能にしている。孔を開けた周囲のデザインを工夫したことも場合により有効である。

【0041】請求項18記載の発明では、請求項1〜請求項12いずれかに記載のセキュリティシステムで、撮像の時刻情報が撮像データに組み込まれることを特徴としている。

【0042】すなわち請求項18記載の発明では、撮像の時刻情報が撮像データに組み込まれること、泥棒等の無断侵入や盗難あるいは不正行為の起きた日時を推測する可能性が高くなる。また、子供が学校から帰ってきた時間等も簡単に知ることができる。

【0043】請求項19記載の発明では、請求項1、請求項3、請求項5、請求項7、請求項9、請求項11いずれかに記載のセキュリティシステムで、撮像データ記憶手段は画像を順次1枚ずつ記憶し、予め定められた枚数に到達したときには古い画像から順に上書きして記憶することを特徴としている。

【0044】すなわち請求項19記載の発明では、記憶手段に静止画の画像データを1枚ずつ記憶する場合には、ある程度のメモリ容量に対して古い画像から順に上書きして記憶することで、メモリ不足を解消することができ、特別の事件が起きた時点で画像データを確実に再現することができる。

【0045】請求項20記載の発明では、請求項2、請求項4、請求項6、請求項8、請求項10、請求項12いずれかに記載のセキュリティシステムで、前記した所定の受信先は予め定めた携帯端末等の通信端末であることと特徴としている。

【0046】すなわち請求項20記載の発明では、携帯端末を受信先とすることで迅速な対応が可能になる。ま

た撮像側に音声の入出力装置を備えることで、訪問者との会話も可能になる。

【0047】請求項2記載の発明では、請求項2、請求項4、請求項6、請求項8、請求項10、請求項12いずれかに記載のセキュリティシステムで、前記した所定の受信先は、駐輪場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されることを特徴としている。

【0048】すなわち請求項2記載の発明では、所定の受信先が駐輪場あるいは駐車場等に設けられた集中管理用の通信端末であり、それぞれの発信元ごとにデータが管理されれば、安価に盗難やいたずらの防止が可能になる。

【0049】請求項2記載の発明では、(イ)人の出入りするための扉と、(ロ)この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、

(ハ)この撮像手段を動作させるトリガ手段と、(ニ)扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、(ホ)この撮像データ発信手段の発信に基づく受信先との通信中に受信先から開錠を指示する信号が送られてきたとき扉を開錠する開錠手段とをセキュリティシステムに具備させる。

【0050】すなわち請求項2記載の発明では、撮像データを扉の配置されている側から所定の受信先に発信し、この通信中に受信先から開錠を指示する信号が送られてきたとき扉を開錠するので、扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判断することができる。しかも、第三者の発呼によって開錠すると異なるので、セキュリティを高度に保持することができる。

【0051】請求項2記載の発明では、(イ)人の出入りするための扉と、(ロ)この扉あるいはその近傍に埋め込まれ扉の前の被写体を撮像する撮像手段と、

(ハ)この撮像手段を動作させるトリガ手段と、(ニ)扉あるいはその近傍に埋め込まれ、このトリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する撮像データ発信手段と、(ホ)この撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送する転送手段と、

(ハ)この撮像データ発信手段の発信に基づく宛先との通信中にその宛先から開錠を指示する信号が送られてきたとき扉を開錠する開錠手段とをセキュリティシステムに具備させる。

【0052】すなわち請求項2記載の発明では、撮像データ発信手段の受信先に撮像データを発信できないとき、予め定めた宛先にこれを転送し、その転送先がこれによる通信を行っている場合に限り遠隔操作による開錠を可能にしたので、本来の受信先の都合によって扉を

開けるまでの待ち時間が長くなりたり不可能となるといった事態が発生しない。また、本発明の場合にも扉の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の適否を的確に判断することができる。しかも、第三者の発呼によって開錠すると異なるので、セキュリティを高度に保持することができる。

【0053】請求項2記載の発明では、請求項3～8いずれかに記載のセキュリティシステムで、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備することを特徴としている。

【0054】すなわち請求項2記載の発明では、撮影を行うための孔の工作を行って撮影を妨害するような場合に警報音を出力することにしたので、このような場合を効率的に排除することができる。

【0055】請求項2記載の発明では、請求項3～8いずれかに記載のセキュリティシステムで、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の宛先に送出する警報データ送出手段を具備することを特徴としている。

【0056】すなわち請求項25記載の発明では、撮影を行うための孔の工作を行って撮影を妨害するような場合に警報を示すデータを所定の宛先に送出する警報データ送出手段を具備させたので、家屋の侵入や自動車等の盗難等が行われる際にこれを所有者等の所定の者に迅速に知らせることができるようになる。

【0057】請求項26記載の発明では、請求項3～8いずれかに記載のセキュリティシステムで、孔は複数配置されており、トリガ手段は、障害検出手段が1つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を動作させることを特徴としている。

【0058】すなわち請求項26記載の発明では、撮影を行うための孔を複数配置し、障害検出手段が1つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を動作させることとしたので、撮影の妨害を行う者が1つの孔を塞ぐ等の行為を行っても、他の孔を通じて画像を取得することができ、セキュリティを向上させることができる。

【0059】請求項27記載の発明では、(イ)交通機関の走行のための動力源が始動されたときこれを検出する動力源始動検出手段と、(ロ)この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関の所有者の所持する特定通信端末が存在するか否かを通信によって判断する特定通信端末有無判別手段と、

(ハ)この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対して前記した交通機関の動力源が始動されたことを無線で通知する通知手段とをセキュリティシステムに具備させ

る。

【0060】すなわち請求項27記載の発明では、交通機関を走行させる者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実を鑑みて、動力源始動検出手段が何らかの操作で動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者による交通機関の無断走行等に対処することにしたものである。なお、その通知後の交通機関については、走行を停止させたり、所定の速度以上の速度が出ないようにすることも特定通信端末からの制御が可能である。運転席等のドアをロックして運転を試みた者が車外に逃げ出すまでの時間を稼ぐことも可能である。もちろん、一度このような措置を行った者は、その後、運転できない状態を解除したり、ドアのロックを解除することができる。このような操作は、特定通信端末に割り振られたキースイッチを操作することによって簡単に実現することがきる。

【0061】請求項28記載の発明では、(イ)交通機関の走行のための動力源を作動させるキーを挿入するキー挿入口と、(ロ)このキー挿入口にキーが挿入され前記した動力源が始動されたときこれを検出する動力源始動検出手段と、(ハ)この動力源始動検出手段が動力源の始動を検出したときその周囲にその交通機関のキー所有者の所持する特定通信端末が存在するかを通信によって判別する特定通信端末有無判別手段と、(ニ)この特定通信端末有無判別手段がその特定通信端末が存在しないと判別したときその特定通信端末に対してその交通機関の動力源が始動されたことを無線で通知する通知手段とをセキュリティシステムに具備させる。

【0062】すなわち請求項28記載の発明では、交通機関を走行させるためのキーを所持する者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実を鑑みて、動力源始動検出手段がキーの操作による動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者によるキーを用いた交通機関の無断走行等に対処することにしたものである。なお、その通知後の交通機関については、走行を停止させたり、所定の速度以上の速度が出ないようにすることも特定通信端末からの制御が可能である。

【0063】請求項29記載の発明では、請求項27または請求項28記載のセキュリティシステムで、交通機関の運転席あるいはその近傍を撮像する撮像手段を備え、通知手段はこの撮像した画像を添付して特定通信端末にこれを送信することとを特徴としている。

【0064】すなわち請求項29記載の発明では、たとえばキー挿入口の近傍等の第三者が気づきにくい位置等に撮像手段を配置しておけば、これらの者が不正に運転を試みた場合にその者の画像を特定通信端末に送信する

ことが可能になる。また、家族がその交通機関を運転しようとしていたような場合には、画像を見ることによって第三者が不正に操作しているものでないことを簡単に確認することができる。

【0065】請求項30記載の発明では、請求項27または請求項28記載のセキュリティシステムで、通知手段の通知に基づいて前記した特定通信端末から交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行う交通機関側制御手段を具備している。

【0066】すなわち請求項30記載の発明では、交通機関が高速あるいは長時間運行することで、行方をくまもらし不正に運転を行った者が運転席から逃げるような事態の発生も防止している。特定通信端末では必要に応じてこのような措置を解除する電波を送信することもできる。

【0067】

【発明の実施の形態】

【0068】

【実施例】以下実施例につき本発明を詳細に説明する。

【0069】第1の実施例

【0070】図1は本発明の第1の実施例におけるセキュリティシステムの構成の概要を表わしたものである。家屋111のドア112にはドアノブ113が取り付けられており、その下のドア部分にはキーホール114が設けられている。ドアノブ113の上側のドア部分には撮像用孔115と照明用孔116が開けられている。このセキュリティシステムでは、来訪者117がドア112のところで来て、ドアノブ113に手を触れれば、照明用孔116に内部から埋め込まれた赤外線LED（発光ダイオード）ランプ118が発光して、撮像用孔115の内部に配置された撮像素子（2次元CCD）が来訪者117を撮影するようにになっている。本実施例ではキーホール114が施錠用に使われる。

【0071】図2は、ドアの要部を断面で示したものである。この実施例のドア112の外側に取り付けられているドアノブ113と内側に取り付けられているドアノブ121とは機構的に連動していない比較的簡易なタイプのものである。撮像用孔115はドア112の内側面貫通しており、内側から画像ユニット122の筒状部122Aが嵌入されるようになっている。筒状部122Aは、ドア112の外側に面した箇所に単一あるいは複数枚のレンズから構成される光学レンズ123を配置しており、その焦点位置にデジタルカメラ等に広く使用されている2次元イメージセンサとしてのCCD（Charge Connected Diode：電荷結合素子）124を配置している。

【0072】画像ユニット122の筒状部122Aには画像出力部122Bが取り付けられており、この部分は

ドア112の内側の面に接着されている。画像ユニット112は一体構造となっているので、ドア112の外側からこれを取り外すことができないようになっている。CCD124と画像出力部122Bの間の空間には、CCD124から出力される画像を処理する画像処理回路125と、画像データを蓄積するメモリ126が収容されている。画像出力部122Bは、ドア112の内側から所望の時点で撮影を行うためのスイッチ127と、画像データを読み出すための画像データ出力端子128と、外側の画像あるいは蓄積された画像を表示する液晶ディスプレイ129から成っている。

【0073】このうちCCD124には、たとえば640×480ピクセルのカラー画像を記録することができるものが使用されている。用途によっては更に高解像度のものを用意することもできる。画像処理回路125はCCD124から得られた画像データをメモリ126に記録するための画像処理を行うが、これと共に画像ユニット122全体の制御も行うようになっている。すなわち、画像ユニット112はドアノブ113および赤外線LEDランプ118と接続されており、ドアノブ113の電位変化を検出して、来訪者117がドアを開けようとこれに触れたときに赤外線LEDランプ118を発光させる。これと共にCCD124は被写体の画像を1枚あるいは予め定めた時間間隔で所定枚数撮影するようになっている。撮影によって得られた画像データはメモリ126に記憶される。赤外線LEDランプ118の発光が気がついて来訪者117がこれに目を向けるようなことがあれば、本人を特定するのに特に好都合な画像を取得することができる。

【0074】メモリ126はたとえば16メガバイト〜128メガバイトの容量を持っている。たとえば16メガバイトのメモリ容量の場合には、640×480ピクセルのカラー画像を撮影日時を合成して150枚程度記憶することができる。メモリ126は画像処理回路125の制御の下で規定枚の画像データを記憶していき、これを超える画像データが入力される時点から古いものを1枚ずつ消去して、新しい画像データに置き換えるようにしている。

【0075】画像ユニット112には、図示しない電源回路から電源が供給されるようになっている。電源回路はドア112に直接、商用電源あるいはこれを直流に変換した後の電源を引き込むようにしてもよいが、ドア112は開け閉めが行われるので、ヒンジ部分の電線の耐久性が問題となる。そこで本実施例のセキュリティシステムではドア112が閉まっている状態でドア112の内側表面に配置された図示しない受取器具と接触する屋内電源側器具とが電磁結合を行って、電気エネルギーをドア112内部の電源回路に供給するようになっている。この電源回路の内部には同じく図示しない容量の比較的大きなコンデンサあるいは二次電池が配置されてお

り、画像ユニット112や赤外線LEDランプ118等の各部を駆動するための電源を供給するようになっている。もちろん、ドア112の内側から乾電池をセットしておくことも可能である。

【0076】画像出力部122Bにはスイッチ127が付属しており、これを押すことによりCCD124を起動して、これによって得られた画像を表示すると共に、その画像をドアノブ113による検知の場合と同様にメモリ126に書き込むようになっている。画像データ出力端子128は、必要に応じてメモリ126内に格納されている画像データの読み出しを行う際に使用する出力端子である。この出力端子あるいはスイッチ127を操作しても、メモリ126の内容を消去することはできない。これは、家庭111（図1）に無断で侵入した者が画像を勝手に消去する事態の発生を防止するためである。したがって、スイッチ127が短時間内に押される回数を制限したり、1日に押される回数の上限を設けるようにすることも、一度撮影された画像を侵入者が勝手に上書きして消去する事態を防止するためには有効である。

【0077】もっとも、このセキュリティシステムの最大の効果は、画像が撮像されて記録されることに気がついた侵入者等が、家屋への侵入等の所期の目的を達成することを断念して早期に立ち去るという犯罪の抑止効果にある。キーホール114に鍵を開ける道具を差し込んだ後、あるいは差し込む前にドアノブ113に手を触れたとき、赤外線LEDランプ118が発光するが、これに気づいた段階でその来訪者117の画像はすでに撮影されており、鍵をさすって開ける前にその場から早々と立ち去らざるを得なくなるからである。夏等に風通しを良くするために、ドア112を少し開けているような場合にも、これを押しかけて入ろうとする時点ですでに撮影が行われてしまう。

【0078】もちろん、家人も出入りの度に撮影される訳であるが、当人の場合には、撮られた画像が他人に利用される訳でもないで、何ら問題とならない。それどころか、子供が学校から一度帰って遊びに行ったのか、まだ全然帰って来ないのかというようなチェックが可能になる。また、留守をしているときに友人が訪ねてきたような場合にも、これを確認することができる。

【0079】なお、実施例では来訪者117の検出をドア112の電位変化によって行っているが、光の反射あるいは遮断を検出する等の慣用の手法を用いて来訪者117を検出するようにしてもよい。また、呼び鈴やインターホン（ドアホン）が押されたときこれによって来訪者が来たことを判別して撮影を行うようにしてもよい。また、実施例では撮像ユニット115と照明ユニット116を設けたが、キーホールに似せた孔を設け、これらの内部にこのような部品をセットしてもよい。マイクロフォンやスピーカを配置する場合についても同様である。

【0080】以上説明した本実施例では、既存のアパート等の家に家主等が僅かの費用をかけるだけで、高価な特殊な鍵を取り付ける以上の防犯効果を得ることができる。また、実施例では赤外線LEDランプ118を撮影に使用しているが、通常のLED等の照明手段でもよい。また、周囲が明るい場所では照明用のランプを使用せずに撮影を行うことができる。また、長期に不在になるような場合には、通常のストロボのような発光がより明瞭に外部から分かる照明手段を使用することも有効である。

【0081】第1の実施例の変形例

【0082】図3は、本発明の第1の実施例の変形例としてのセキュリティシステムを屋内から見たものである。第1の実施例の図2と同一部分には同一の符号を付しており、これらの説明を適宜省略する。この変形例のセキュリティシステムでは、図示しないコンセントに接続された電源送信装置142がドア112側に取り付けられた電源受信装置141に電磁結合によって電源を供給している。電源受信装置141に接続された画像記録ユニット123A内には先の実施例のような大容量のメモリは内蔵されておらず、撮影した画像は、画像記録ユニット123Aに取り付けられたアンテナ143から屋内の所定の箇所に隠された受信装置144で受信され、ここで比較的大容量のメモリに順次格納されるようになっていく。

【0083】したがって、撮像装置に気がついた侵入者がドア112の全部または一部を壊すことによって画像記録ユニット123Aを破壊させたり、これを持ち去ることがあっても、その者の画像を安全に退避させることができる。また、受信側が比較的大容量のメモリを備えていれば、動画や高解像度の画像を充分な量、通信によって蓄えることができる。

【0084】なお、画像記録ユニット123A自体が携帯電話機等の無線端末に画像等のデータを直接配信することも可能であるし、受信装置144に所定のモード設定を行ったときにはこれが中継する形で携帯電話機等の無線端末に画像等のデータを配信するようにしてもよい。これにより、留守中の自宅に誰かが訪問するたびに、携帯電話機等でこれを把握することができる。したがって、画像記録ユニット123A側にマイクロフォンやスピーカを配置しておけば、その者と必要な会話をすることも可能になる。

【0085】第2の実施例

【0086】図4は、本発明の第2の実施例におけるセキュリティシステムの構成の概要を表わしたものである。本実施例で図1と同一部分には同一の符号を付しており、これらの説明を適宜省略する。

【0087】本実施例ではドア112に改造を行うことが困難な者を対象にして、その付近の物品に来訪者の画像を撮影する装置を組み込むことにしている。この例で

は郵便ポスト161をそのための装置としているが、新聞入れ、呼び鈴あるいはドアホンのような物であってもよい。

【0088】図5は、この例の郵便ポストの構成を示したものである。郵便ポスト161は郵便投函口162をその上部に有し、下部には郵便回収口163を有している。郵便回収口163には、必要に応じてキー164が取り付けられている。郵便ポスト161の郵便投函口162と郵便回収口163の間には、第1～第3の孔166～168が穿たれている。第1の孔166には赤外線LEDランプ118が取り付けられている。第2の孔167の内部には受光素子169が配置されている。第3の孔168の内部には、図示しないレンズと撮像素子が組み込まれている。これらは郵便ポスト161内部の画像処理ユニット171に接続されている。画像処理ユニット171は、郵便ポスト161内部の電池172から電源の供給を受けるようになっているが、可能であれば商用電源から電源を供給することもできる。画像処理ユニット171には送信アンテナ173が付属している。

【0089】このような第2の実施例のセキュリティシステムでは、赤外線LEDランプ118が常時、あるいは間欠的に点灯し、受光素子169が受光レベルを検出することで郵便ポスト161の前に物体が現れたことを検出する。来訪者117があったような場合には、受光素子169がこれを検出し、画像処理ユニット171は前記した撮像素子を駆動して郵便ポスト161の前の画像を1枚ないし所定の時間間隔で複数枚取り込む。そして画像を1枚ずつ送信アンテナ173から送信する。

【0090】送信された画像は、第3の実施例の変形例として図3で説明したと同様に家屋111内の受信装置144で受信され、ここで比較的大容量のメモリに順次格納されるようになっていく。このとき、受信の日付も記録される。したがって、来訪者117が悪意を持った者のような場合で、何らかの異変に気付いて郵便ポスト161を破壊したり、あるいはこれを持ち去るようなことがあっても、来訪者117の画像が記録されているので、これに迅速に対処することができる。

【0091】第3の実施例

【0092】図6は、本発明の第3の実施例におけるセキュリティシステムの構成の概要を表わしたものである。この第3の実施例では金庫のセキュリティシステムを扱っている。金庫181はその扉182あるいはその周囲に第1および第2の孔183、184が穿たれている。また、金庫181の背後の部分には送信アンテナ185が取り付けられている。送信アンテナ185は金庫の外側のパネルを一部領域だけ非金属材料としてこの内部に組み込んでおいてもよい。これにより、送信アンテナ185を事前に破壊するという行為を防止させることができる。

【0093】本実施例では第1および第2の孔183、

184の一方に赤外線LEDランプ等の発光手段を配置し、他方の孔の内部に光学系と撮像素子を配置している。また、金庫181の内部には第2の実施例で説明したと同様の画像処理ユニット186が内蔵されている。本実施例の画像処理ユニット186の場合には、電源供給用のコンセント187が備えられているが、金庫181の内部に充電電池188が備えられているので、停電あるいはコンセント187が引き抜かれた場合にも所定時間の間は画像処理ユニット185に電源が供給されるようになっている。

【0094】本実施例のセキュリティシステムの場合にも、所定の安全な場所（複数箇所であってもよい。）に配置された受信装置144（図3参照）が画像データを受信するようになっている。先の実施例と異なるのは、画像処理ユニット186は被写体を検知することなく、たとえば1分間隔で画像データを撮影している。これにより、1日の間に1500枚ほどの画像が撮られて送信アンテナ185から順次受信装置144に送られることになるが、解像度を高くしてもこれらを格納する記憶媒体の容量はごく僅かで足りる。したがって、簡易な受信装置144で画像の管理を充分行うことができる。もちろん、コンピュータを使用して画像データを取り込むようにすれば、画像処理結果と連動した更に高度のセキュリティシステムを構築することができる。

【0095】第3の実施例の第1の変形例
【0096】図7は第3の実施例の第1の変形例として公衆トイレの防犯用のセキュリティシステムを表わしたものである。公衆トイレ201の男女別の入り口202、203の上には蛍光灯等の照明装置204、205が点灯しており、入り口202、203の複数箇所には撮影用の孔206～209が開けられている。これらの孔206～209の内部には前記したようなレンズと撮像素子が配置されている。また、公衆トイレ201の屋上等の所定の位置には送信アンテナ211が配置されていて、その電波が携帯電話機の無線基地局で逐次受信されるようになっている。役所等の公衆トイレ201の管理者側に備えられた記憶装置には、各所に配置された公衆トイレ201の画像データが逐次格納されている。

【0097】もちろん、公衆トイレ201側に比較的大きなメモリ容量の記憶装置を配置して、これに画像データを順次蓄積するようにしたり、30分とか1時間おきにこれらの画像データを無線基地局経由で公衆トイレ201の管理者側へとまとめて送信することも可能である。

【0098】第3の実施例の第2の変形例
【0099】図8は第3の実施例の第2の変形例としてエレベータの防犯用のセキュリティシステムを表わしたものである。エレベータ231の出入り口あるいはその近傍に撮影用の孔232、233を開けておき、その内部にレンズと撮像素子等を配置しておくことで、無断侵入者を撮影し、間接的に無断侵入を防止することができる。

る。画像の撮影は昇降用のボタン234の押下によって準備段階に移行し、ドアが開いて閉まるまでの時間について所定間隔で撮影を行うようにすればよい。エレベータ231の出入り口と対向する壁等にも撮像素子等を配置しておけば、事件があったような場合などのような人物が何層から乗り込んで何階で降りたという事実を特定することができる可能性が高くなる。

【0100】第4の実施例

【0101】図9はドアノブを使用したセキュリティシステムの要部を表わしたものである。第1の実施例のセキュリティシステムと異なるのは、ドア112の外側と内側でノブ251、252が連動したドアノブ253に本発明を適用している点にある。ドアノブ253はドア112と接触する部分に、押さえプレート255、256という金属板（台座）を取り付けるようになっている。したがって、押さえプレート255、256で隠れるだけの大きさの比較的大きな穴をドア112に開け、ドア112の外側に対応した押さえプレート255の背後に取り付けられた画像撮影処理ユニット257をドア112の内部空間に配置するようにする。画像撮影処理ユニット257は、キーロック機構260の存在しない空間を利用して配置されている。

【0102】画像撮影処理ユニット257の取り付けられた押さえプレート255には第1および第2の孔258、259が開けられている。第1の孔258には赤外線LEDランプ等の発光手段が組み込まれており、第2の孔259の背後の画像撮影処理ユニット257内には、図示しないレンズと撮像素子が組み込まれている。もう一方の押さえプレート256には、画像データ出力端子261が埋め込まれている。このような端子の代わりに画像撮影処理ユニット257内に画像データ送信用のアンテナが付属していてもよい。画像データ出力端子261を画像データの出力用に使用する画像撮影処理ユニット257は、画像データのある程度蓄積する必要があるので、その内部に比較的大容量の不揮発性のメモリが配置されている。この点では第1の実施例と同様である。

【0103】画像撮影処理ユニット257の電源は、前記した実施例と同様に電磁誘導によって外部の電源からエネルギーを受け取る電源受信装置262から得ることができる。もちろん、ドア112に何かの用途で電源が供給されている場合にはこれを使用することも可能である。

【0104】本実施例のセキュリティシステムの最大の特徴は、通常の家庭あるいはマンション等に多用されている形式のドアノブを用いるので、新築の際にこれを使用して簡易にセキュリティシステムを実現することができるだけでなく、本実施例のドアノブ253を購入して、今まで使用していたドアノブと交換するだけでセキュリティシステムを導入することができる点にある。特

に無線で画像データを送信するタイプのものでは、携帯電話等の通信端末に訪客者の画像を送信することができ、また、すでに説明したようにマイクロフォンやスピーカを配置しておけば、その者と必要な会話を行うことも可能になる。

【0105】しかも、鉄等の金属で作られた通常のドアは防犯用に加工すること自体が困難であり、また美観を損ねる結果を招来することが多いが、本実施例のセキュリティシステムでは、ドアノブ253を交換するので、美観を損ねるおそれがない。

【0106】第4の実施例の変形例

【0107】図10は、本実施例を自動車に応用したセキュリティシステムの概要を表わしたものである。自動車281もその外部が金属で作られており、防犯用に特別に加工すると美観を損ねるおそれがある。しかしながら、ドア282、283を開けるときに必要なドアの把手284、285自体に直接、あるいはドアの把手284、285の付属装置286、287にすでに説明したような孔を開けておき、この部分を使用してドア282、283を開ける人を撮影するようにすれば、ドアの把手284、285あるいはその付属装置286、287を交換することでセキュリティシステムを導入することができる。

【0108】この変形例の場合にも、自動車281に近接し、あるいはドアの把手284、285等に接触した時点で、あるいは所定の時間間隔でドアの把手284、285の近傍の画像が1枚ずつ撮られるので、自動車281の盗難は事実上困難になる。画像データを自動車281内部に蓄積するか、図7で説明したような無線を使用して所定箇所に送信するかは自由であるが、自動車281自体を盗まれた場合を想定すると、無線を使用して画像を携帯電話機や所定の管理サーバ上に送信しておく方が有効である。

【0109】またこの変形例ではドアの把手284、285あるいはこれらの付属装置286、287の内部に撮像素子等を配置することにしたが、バックミラー等の他の部品の内部に撮像素子等を配置することができれば、同様に本発明を適用することができる。また、鍵自体がドアの把手284、285自体に取り付けられていないような場合には、その鍵と一体的に撮像素子等を配置することも可能である。

【0110】第5の実施例

【0111】図11は本発明の第5の実施例のセキュリティシステムの概要を表わしたものである。このシステムは、自転車301、自動車302、バイク303等の各種交通機関を駐車する駐車場（もちろん、自動車302とか自転車301のいずれか1種類の交通機関のみを駐車するものは駐輪するものであっても可能。）で使用されるものである。この例で自転車301、自動車302、バイク303は、それぞれ先の実施例の変形例で説

明したドアの把手やボディの所定箇所あるいはハンドル、外付けのスピードメータ等に人の接近や接触を検知する検知手段と撮像装置を備えている。駐車場304には、これらの交通機関で共通使用される受信装置305が設置されている。駐車あるいは駐輪している自転車301、自動車302、バイク303等の各種交通機関は人の接近や接触を検知すると、自己のIDと共に撮影した画像データを受信装置305に送信するようにしている。受信装置305は比較的大容量のメモリを備えており、受信した画像データをID別に区分けして記憶するようにしている。

【0112】したがって、盗難やいたづらが発生すると、駐車場304の管理者に通知して画像を読み出してもらうことにより、事故の発生日時とこれに係わった可能性のある人物の画像を入手することができる。もちろん、受信装置305を介して所有者の通信端末に必要な画像を中継する契約を行うことも可能である。

【0113】同様のシステムは、ボート等の船舶や集合住宅を管理する場所でも適用することができる。また、インターネットを利用してウェブ・サーバで一括管理することもできる。

【0114】第6の実施例

【0115】図12は本発明の第6の実施例のセキュリティシステムの概要を表わしたものである。ここでは、絵画の展示場で適用されるシステムを表わしている。それぞれの絵画321、322の前には鑑賞者323の接近を検知してその画像を撮影し送信する撮像送信ユニット324が取り付けられている。撮像送信ユニット324は、壁に直接埋め込まれていてもよい。各撮像送信ユニット324の送信した画像データは館内の受信装置325が受信して、その比較的大容量のメモリにサイクリックに書き込んで、容量が満ちた時点で古い画像を上書きするようになっている。入場者が多い場合には、30秒おきというように所定の時間間隔で画像データを読み込んで送信するモードに設定しておいてもよい。また、異常な行動（画像の動き）が管理者側あるいは画像の差分データをとる装置等で察知された場合には、画像を高解像度に切り替えたり、動画モードに切り替えるようにしてもよい。

【0116】このように本発明はドアあるいは扉に用途が限定されるものではなく、動産全体、不動産の一部としての所定の空間あるいは道路に対しても適用することができる。撮像された画像は順次格納しておき、メモリ容量が少ないときには古い画像データに上書きしていくようにすることで、システムの有効性を高めることができる。しかも悪意の者が撮影に気付いたときにはすでにその画像が安全な場所に格納されていたり、遠隔地等に送信されているので、所期の目的を達成させることなく退散させるといった効果がある。

【0117】第7の実施例

【0118】図13は本発明の第7の実施例のセキュリティシステムの概要を表わしたものである。この図で図1と同一部分には同一の符号を付しており、これらの説明を適宜省略する。本実施例では、ドア112に電子式錠装置401が取り付けられており、その上部にセキュリティ装置402が取り付けられている。電子式錠装置401にはドア403とキー溝404が取り付けられている。電子式錠装置401はキー溝404に差し込み指示しないキーによって開錠することができる。セキュリティ装置402の指示によっても開錠することができるようにしている。

【0119】本実施例のセキュリティ装置402は後に説明するように独自のアドレスを有する無線端末としての機能を有しており、最寄の基地局411に対して発呼できるようにしている。ただし、基地局411を介して他の無線端末あるいは固定式電話等の端末から発呼することはできない。すなわち、セキュリティ装置402は自ら発呼して接続した端末との間でみ通話やデータの交換を行うことができる。これは、セキュリティ装置402が悪意の第三者の指示によって電子式錠装置401に開錠の指示を与えることを防止するためである。

【0120】基地局411は通信網412を介して他の基地局413（図で代表的に1つのみを表示している。）やセキュリティ管理会社414と接続されている。図ではセキュリティ管理会社414が通信網と有線と接続されている形を示しているが、無線で接続されていてもよいし、インターネット網等の他の通信網を介して接続されていてもよい。ここで携帯電話端末415はセキュリティ装置402の所持者の端末であるとする。

【0121】図14は、本実施例のドアの要部の断面構造を表わしたものである。ドア112に組み込まれたセキュリティ装置402は、図2で示した実施例のように単一あるいは複数枚のレンズから構成される光学レンズ123と、2次元イメージセンサとしてのCCD124を備えている。また、光学レンズ123の上方にはスピーカ部421が配置され、下方にはマイク部422と赤外線LEDランプ118が配置されている。スピーカ部421、マイク部422および赤外線LEDランプ118の後側のスペースには制御部423が配置されている。制御部423は画像処理だけでなく、通信制御や音声の入出力および電子式錠装置401の制御も行うようになっている。セキュリティ装置402の背後には無線アンテナ425が取り付けられており、また電子式錠装置401の間には制御信号線426が取り付けられている。セキュリティ装置402の電源は、図3に示した第1の実施例の変形例のようにして取得してもよいし、電子式錠装置401から図示しない電源ラインを使用し取得してもよい。なお、無線アンテナ425は図14に示したようにドア112内部に配置してもよいし、他の場所まで無線用の信号線を延長して、電波の送受信に

良好な場所に配置するようにしてもよい。

【0122】図15は、本実施例における電子式錠装置の開錠制御の様子を表わしたものである。本実施例では、たとえば幼少の子供が家に帰ってきたときに親等がこれを確認して、家の内部に入るための鍵を開けることができる。店の従業員を確認後に店内に入ったり、来客が来る予定のときに突然来訪してしまい、とりあえずその来客を家または事務所の内部に通ずる場合には本実施例が有効である。本実施例ではこれらの者を他の実施例と同様に来訪者117と総称する。

【0123】図13または図14に示したセキュリティ装置402あるいは他の周知の装置がドア112の付近に現れた来訪者117を検知すると（ステップS451:Y）、撮影を行った後、「撮影を行わせていただきます」等の音声スピーカ部421から流れて（ステップS452）、悪意の来訪者を立ち退かせる処置が行われる。この後に再度、来訪者117がドア112の前にいるかどうかを検知して（ステップS453）、いなくなれば（Y）、処理を終了させる（エンド）。

【0124】この状態でも来訪者117が依然として検知されていれば（ステップS453:N）、図14に示した制御部423は予め指定したその家の主人等の携帯電話機等の携帯電話端末415へ発呼する（ステップS454）。その後、時間 t_1 以内に指定端末としての携帯電話端末415との通話が可能になれば（ステップS455:N、S456:Y）、その携帯電話端末415から開錠を指示する信号が到来した時点で（ステップS457:Y）、制御部423は開錠指示信号を制御信号線426を介して電子式錠装置401に送り、開錠処理を行う（ステップS458）。この場合、電子式錠装置401は所定時間経過後に再び自動的に施錠する。その携帯電話端末415が開錠を指示するには、所定のパスワードを入力することを条件にしてもよい。開錠指示信号が到来することなく通信が終了した場合には（ステップS459:Y）、一連の処理が終了する（エンド）。

【0125】なお、携帯電話端末415の所有者は、開錠指示信号を送信する前にCCD124の画像を受信しており、またスピーカ部421やマイク部422を通じて来訪者117と会話して、開錠を行う必要のある者であるかどうかを十分確認することができる。また、単なるセールスマン等の開錠を行う必要のない者に対しては、通話によって必要な処理を行うことができる。

【0126】一方、子供が家に帰ってきて鍵を開けてもらうような場合に、携帯電話端末415の所有者がたまにたまに（着呼できないときも含む）、その所有者が転送モードを設定しているかどうかを確認する（ステップS460）。転送モードに設定されていない場合には

(N)、一通の処理が終了する(エンド)が、設定されている場合には(Y)、図13に示したセキュリティ管理会社414へその通話先が変更される。なお、セキュリティ管理会社414への転送の前に、母親の代わりに父親の携帯電話機というように他の者に転送が行われるようにしてもよい。

【0127】セキュリティ管理会社414が着呼すると(ステップS461)、先の携帯電話端末415の所有者と同様に専門のスタッフが来訪者117と通話を行ったり、画像を確認して、予め指定された子供のように聴かぬ者に対しては開錠信号を代行して発信する。セキュリティ装置402は、開錠信号が到来したら(ステップS462:Y)、すでに説明したように開錠処理に進み(ステップS458)、通信が終了したら(ステップS463:Y)、すべての処理を終了させることになる(エンド)。

【0128】なお、セキュリティ管理会社414は開錠の処理を行ったり、来訪者と話をしたような場合には、これを電話で携帯電話端末415の所有者に通知したり、その内容のメールを出すことも有効である。

【0129】このように本実施例ではセキュリティ装置402が発呼したその通話中に開錠信号が到来したときのみ、このセキュリティ装置402から電子式錠装置401に対して開錠の指示がでる。したがって、他の場所から開錠を指示する信号を送って開錠を行う場合と異なり、セキュリティが極めて高くなる。しかも来訪者117は撮影されるので、この点でも悪意の来訪者に対するセキュリティが高い。

【0130】図16は、悪意の来訪者が撮影を妨害する場合の対策としての処理の流れを表わしたものである。この処理は、本実施例に限らず先の各実施例でハードウェアを工夫することで同様に行うことができる。図14に示したCCD124は時間ごとドア112の前を撮影している(ステップS471、S472)。そして、撮影が行われるたびに特定の複数の画素から得られる画像の明るさ、あるいは全体の画像の明るさを前回のもの、あるいは前回の複数回分のものと比較するようにしている(ステップS473)。比較された結果、明るさの差が予め定めた許容値以内の場合には(ステップS474:Y)、特に異常が発生していないものとしてステップS471の処理に戻る。

【0131】ところで、悪意の者が自分が撮影されるのを嫌って、図14に示す光学レンズ123にガムテープのようなものを貼り付けて撮影ができないようにすることが考えられる。このような場合には、CCD124に到達する画像の明るさが急激に減少する。また、人によっては懐中電灯等の光の出るものをCCD124の前に配置して、明るさを維持しながら犯行を企む場合がある。更に光学レンズ123を破壊するようなこともある。このような場合には、いずれにせよCCD124が

得る画像の明るさが変化する。

【0132】このように明るさの差が予め定めた許容値を越えるような場合には(ステップS474:N)、制御部423はスピーカ部421を制御して警報音を所定時間、たとえば10秒間出力する(ステップS475)。この後に、再度、CCD124による撮影が行われる(ステップS476)、その画像の明るさが基準値の範囲内であるかどうかのチェックが行われる(ステップS477)。ここでの基準値の範囲はステップS474の範囲であってもよいし、ステップS474の処理による誤動作を防止するために予め設定されている値の範囲内であってもよい。基準値の範囲内であれば(Y)、悪意による撮影の妨害が解消したものととして、ステップS471の処理に戻る。ただし、装置によっては撮影した画像を解析し、ドア112の前の通常得られる画像と異なる場合には「基準値の範囲」外としてもよい。

【0133】ステップS477で基準値の範囲外とされた場合には(N)、セキュリティ装置402が指定端末としての携帯電話端末415に発呼する(ステップS478)。これにより、携帯電話端末415側では音声で通話する等により状況を確かめ、必要に応じて警察に通報する等の措置を採ることができる。携帯電話端末415側が通話をするとかたがたしないような場合にはセキュリティ管理会社414に転送され、あるいはこれを宛先として発呼が行われることも可能である。

【0134】第8の実施例

【0135】図17は本発明の第8の実施例のセキュリティシステムの概要を表わしたものである。このセキュリティシステムは、自動車401の運転席の上方に配置された広角の撮像装置402と、後部座席の上方に配置された温度検出器403、マイクロフォン404、スピーカ405、非常ボタン406および無線送受信器付制御装置407とにより構成されている。このうち、温度検出器403、マイクロフォン404、スピーカ405、非常ボタン406および無線送受信器付制御装置407は1つの筐体内に納められていてもよい。もちろん、撮像装置402も含めて全体を一つの比較的小さな筐体内に格納することも可能である。この場合、携帯電話機にCCD撮像装置と温度検出器が組み込まれたようなものを想定すればよい。

【0136】図18は無線送受信器付制御装置の制御の概要を表わしたものである。無線送受信器付制御装置407は予め定められた1または複数の携帯電話機等の通信端末の受信端末として動作すると共に、特定の場合にはこれら1または複数の携帯電話機等の通信端末に対して所定の優先度をもって発呼できるようになっている。

【0137】前記した1または複数の携帯電話機等の通信端末が発呼して、所定の操作によってモニタ信号を送信してくると(ステップS421:Y)、CPU(中央処理装置)を内蔵した無線送受信器付制御装置4

07は画像・音声通信モードに移行し(ステップS422)、撮像装置402で静止画あるいは動画を撮影してこの通信端末に送信すると共にマイクロフォン404およびスピーカ405を動作状態にして、音声あるいは車内の音を送信状態にすると共に、通信中の通信端末から送られてきた音声信号による音声をスピーカ405から出力する。したがって、その通信端末は車内の者と通話を行うことができる。画像・音声通信モードの解除は、その通信端末がモニタオフ信号を送信してこれが無線送受信器付制御装置407側で受信されることによって行われる(ステップS423)。

【0138】一方、車内の温度が予め設定した温度よりも高い異常な状態になったとき(ステップS424:Y)、あるいは非常ボタン406が押されたとき(ステップS425:Y)、無線送受信器付制御装置407は前記した通信端末に発呼する(ステップS426)。このような通信端末が複数存在する場合には最優先のものに発呼し、これが応答しないときには次の優先順位の通信端末に対する発呼に切り替わる。予め定められた通信端末が3つ以上存在する場合には、接続が行われないたびに順次下位の通信端末に切り替わる。通信端末の中には先の実施例の図13で示したようなセキュリティ管理会社が含まれていてもよい。

【0139】相手の通信端末と通信できる状態になったら、ステップ422に移行して画像が送信され、音声で通話ができる状態になる。この画像・音声通信モードの解除は、通信中のその通信端末がモニタオフ信号を送信することで行われるが、車内の者が図示しないリセットボタンを押せば通信が強制終了する。

【0140】この第8の実施例のセキュリティシステムによれば、たとえば車内に子供が取り残されたり、うっかり置き忘れたような場合で温度が異常に上昇したとき、親等の通信端末が自動的に呼び出され、車内の様子が伝達される。また、車内で何らかの異常が発生したような場合には、非常ボタン406を押すことで車外の者にこれを通知することができる。たとえば強盗が車内に押し入ったような場合には、自分の携帯電話機をオフにして非常ボタン406を押せば、自分の携帯電話機よりも下位の優先順位の親元等に車内の状況を把握させることができる。この意味では特に撮像装置402は車内の目立たない位置に最初から組み込まれていることが望ましい。このような場所のとしては、エアーコンディショナの送風口やスピーカの孔を一例として挙げることができる。

【0141】なお、第7の実施例等では無線で異常等の通信を行ったが、固定式電話機のように有線でこれらの通信を行うことも可能である。また、各実施例ではレン

ズとCCDを1組配置することにしたが、これらを複数組配置するようにしてもよい。この場合には、他人の悪意あるいは装置の故障によりそのうちの1つの撮影ができなくなるような事態が発生しても、撮影を行うことができる。特に、第7の実施例のような構成であれば、1つの撮像系に異常が検出されたときに残りの撮像系で撮影すると共に、必要に応じて所定の優先に連絡を行うことができる。したがって、たとえば自動車の盗難や家屋の侵入といった事態の発生時に迅速に対処することができると共に、有力な証拠を取得することも可能になる場合がある。

【0142】第9の実施例

【0143】図19は本発明の第9の実施例のセキュリティシステムの概要を表わしたものである。本実施例のセキュリティシステムでは、自動車の運転席前方のボード501上におけるキー挿入口502のすぐ上にスピーカの音声出力用の複数の孔の集合体503が配置されている。このうちの中央の比較的大きな孔504の内部には、たとえば第7の実施例で説明したドア112の光学レンズ123およびCCD124の組み合わせからなる撮像装置505が配置されている。また、ボード501内部で撮像装置505の前方あるいは背後には、音声出力用のスピーカ506が配置されている。更に、キー挿入口502の背後には音声を取り取るためのマイクロフォン507およびエンジン始動検出回路508が配置されている。エンジン始動検出回路508は、キーの回転位置を図示しないマイクロスイッチ等の機械的なセンサで検出するようなものであってもよいし、実際にエンジンが始動したことを自動車の制御回路が判別したことに沿って信号をそのまま利用してもよい。

【0144】撮像装置505、スピーカ506、マイクロフォン507およびエンジン始動検出回路508は、同じくボード501の内部に配置された装置内通信端末511と接続されている。装置内通信端末511はカメラ内蔵携帯電話機のカメラを取り除いた本体部分とはほぼ同様の構成となっており、車内の図示しない電源装置から電源の供給を受けるようになっている。この装置内通信端末511はこれを搭載した自動車の所有者の携帯電話機512とは異なった電話番号を有しており、単独で最寄りの無線基地局513ならびにその通信ネットワーク514を経由して予め設定した相手にデータの送信を行うことができるようになっている。

【0145】携帯電話機512は全く通常の携帯電話機であるが、装置内通信端末511と対の関係を持っている。対の関係は、携帯電話機512側あるいは装置内通信端末511から他方の装置に設定するものであり、設定内容は双方の電話機(通信端末)の図示しないROM(リード・オンリ・メモリ)内に格納される。本実施例ではこのように装置内通信端末511と対の関係を持っている携帯電話機512を特定携帯電話機512と呼ぶこ

とにする。

【0146】図20は、本実施例で自動車の所有者あるいは第三者がこの自動車を運転するためにキーを差し込んだ場合の装置内通信端末511の制御の様子を表わしたものである。装置内通信端末511の図示しないCPUは、エンジン始動検出回路508がエンジンの始動を検出すると(ステップS531:Y)、撮像装置505を駆動して運転席でキーを操作した者の画像を記録する(ステップS532)。この画像は比較的短時間の動画であってもよいし、静止画を複数枚撮影するものであってもよい。複数の孔の集合体503に方向を変えて複数の撮像装置505を組み込むことができ、この場合には各種の方向の画像を撮影することができる。したがって、キーを挿入した者を特定する画像をこのうちの幾つかに取めることができる可能性が高い。この意味では運転席を見渡せる位置であってキー挿入口502から比較的離れた位置に更に撮像装置を配置したり、もともと撮像装置を独自の観点から1または複数個、車内の所望の位置に配置しておくことも有効である。

【0147】このようにして画像の撮影および記録が行われたら、CPUはこの自動車の内部または近くに所有者の携帯電話が存在するかどうかを判別する。この判別のために装置内通信端末511は特定携帯電話機512に対して電話を掛ける。そして特定携帯電話機512が同一の無線基地局513の受信エリアに存在する場合には近くにいるものと判別して(Y)、その時点で通話を終了させる(リターン)。したがって、特定携帯電話機512によっては着信音が鳴動する。

【0148】装置内通信端末511は特定携帯電話機512が同一の受信エリアに存在しないことを判別したら(ステップS533:N)、先に撮影した画像を現在の位置情報と共に特定携帯電話機512に対して送信する(ステップS534)。このとき、撮影日時に関する情報も送られる。ただし、特定携帯電話機512がGPS(Global Positioning System: 全地球測位システム)等の位置検出手段を備えていない場合には、撮影した画像とその撮影日時のみが送信されることになる。

【0149】したがって、いずれかの者がキーを用いて無断に自動車のエンジンを始動させた場合には、特定携帯電話機512に対してこの画像やその他のデータが送られてくることになる。自動車の所有者は送られてきた画像によって、これが家族等の正当な権限を有する者の乗車であるかどうかを容易に判別することができる。また、場合によってはこの者とスピーカ506およびマイク507を用いて会話をして確認を行うことができる。

【0150】これにより、その自動車の発進に問題がないとされる場合、特定携帯電話機512の所有者は所定のキースイッチを押下して所定の終了通知を装置内通信端末511に対して送出する。装置内通信端末511は

この終了通知を受信すると(ステップS535:Y)、一連の送信処理を終了させる(リターン)。このような終了通知が受信されない場合、装置内通信端末511は時間tが経過するたびに(ステップS536:Y)、同様に運転席の画像を記録して(ステップS537)、ステップS534に戻りこれを特定携帯電話機512に対して送信する処理を繰り返す。したがって、第三者が勝手にその自動車を発進させたような場合には、その第三者が運転を行っている間、その画像を特定携帯電話機512に対して送信することができる。装置によっては、通信状態を継続させて運転席の画像を順次送信するようにしてもよい。

【0151】なお、本実施例では撮像装置505、スピーカ506、マイク507を配置したが、これらの一部または全部を省略しても特定携帯電話機512に対してその者の所有する自動車が無断に発進される事態を迅速に通知することができる。また、実施例では装置内通信端末511が特定携帯電話機512に対して通常の発信を行ったが、同一サービスエリア内で内線通話を行える場合には内線通話を試みて、通話が成立したときに特定携帯電話機512が近くに存在するものと判別してもよい。

【0152】第9の実施例の変形例

【0153】図21は本発明の第9の実施例のセキュリティシステムの変形例としての特定携帯電話機のセキュリティシステムの要部を表わしたものである。この変形例の特定携帯電話機512Aは着脱自在の近距離通信カード515をセットしている。この近距離通信カード515は所定のIDの値から返答要求があつと、これに対して返答用の電波を自己のIDと共に一定時間だけ出力するようになっている。もちろん、このような近距離通信カード515と同様の機能を有する回路が予め特定携帯電話機512Aの内部に一体として組み込まれていてもよい。

【0154】一方、自動車側にセットされている装置内通信端末511Aは、運転のためのキーが図19に示したキー挿入口502に挿入されてエンジンの始動のための操作が行われたとき、所定時間になつて自己のIDと返答要求を送出するようになっている。この装置内通信端末511Aおよび特定携帯電話機512Aの送出するこれらの電波は遠くまで届くことの無い微弱な電波である。

【0155】図22は、この変形例における装置内通信端末側の処理の流れを示したものである。装置内通信端末511A内の図示しないCPUは、第9の実施例で説明したエンジン始動検出回路508がキーの操作によるエンジンの始動を検出すると(ステップS571:Y)、自己のIDと返答要求信号を送信する(ステップS572)。これらの信号は無線基地局513に送出されるような強い電波ではない。特定携帯電話機512A

がその自動車内あるいはその自動車の近辺に存在する場合にこれらの電波を受信する。そこで、前記したように特定携帯電話機512AはそのIDをチェックして対応関係にある装置内通信端末511Aのものであれば自己のIDを付した返答信号を出力する。この返答信号も無線基地局513に送出されるような強い電波ではない。

【0156】装置内通信端末511Aは、返答信号を受信したら(ステップS573:Y)、これに含まれているIDが装置内通信端末511Aと対の関係にあるものとして予め登録されたIDであるかどうかをチェックし(ステップS574)、登録されたIDであれば一連の処理を終了させる(エンド)。

【0157】これに対して、ステップS573で返答信号が返り返されてこなかったり(N)、あるいは返答信号自体は装置内通信端末511で受信されてもそのIDが登録された内容と一致していなかったような場合には(ステップS574:N)、第三者がキーを操作した可能性がある。そこでこの場合には、装置内通信端末511が特定携帯電話機512Aに対して電話を掛けることになる(ステップS575)。この際に、撮影が行われればその画像を送信してもよいことはもちろんである。

【0158】このようにこの変形例では、自動車のエンジンを始動させるときにその近くに所有者の携帯電話機が存在する場合に無線基地局513を介しての所有者への発信を控えるようにした。このため、自動車の所有者がキーを操作してエンジンを始動させるたびに通信費の出費を強いられるということがなくなる。また、変形例では独自の電波を利用して装置内通信端末511Aが特定携帯電話機512Aの存在の有無を判別するので、その電波の強度や感度を調整することで、装置内通信端末511Aと特定携帯電話機512Aの間の感知できる距離をある程度自在に調整することができる。したがって、実施例ではコンビニエンスストアに買い物に立ち寄った場合に自動車の盗難に合う可能性があるが、この変形例では特定携帯電話機512Aを車外に持ち出した状態で特定携帯電話機512Aの検知できる範囲外とすることができる。

【0159】第10の実施例

【0160】図23は本発明の第10の実施例のセキュリティシステムの要部を突出したものである。この実施例では、先の実施例の図1と同様にドア112におけるドアノブ113の上側に撮像用孔115が配置されているだけでなく、集合住宅における部屋番号や居住者を示したプレート591の透明部分あるいは半透明部分の裏側に別の撮像用孔92が設けられている。これにより、来訪者の背が高かったり、ドアノブ113の位置が比較的低い位置であった場合にも、その者の画像を正確に捕らえる確率が高くなる。

【0161】このように来訪者の顔または姿を画像として正確に捕らえるためには、撮像用の装置のレンズを比較的低角のものにするか、ドアまたはその近辺だけでなく複数の場所から来訪者を捕らえるようにするか、あるいは1つの場所からのみ画像を捕らえる場合にはレンズを複数の場所を向くように光学機構を回転させるといった手法が有効である。光ファイバを使用して複数箇所から得られた画像を1つのCCDに導いてそれぞれの分画領域に画像を結像させ、分割画像として記録することも可能である。

【0162】これに対して、図10に示した自動車のドアの場合には、複数のドアの把手284、285等に対応して撮像装置を配置しておき、1つについて何らかの異常が生じたときに残りの撮像装置も一斉に画像を撮影するようにすると、画像の撮影範囲をある程度重複させておけば、撮影対象をより確実に画像に収めることができる。

【0163】なお、第9の実施例では自動車を例にして説明したが、船舶、ケーブルカー、飛行機等の交通機関であって、その走行のための動力源のオン・オフをキーによって制御するその他の交通機関についても本発明を同様に適用することができる。また、実施例ではキーを用いてエンジンを始動させる場合を説明したが、ボンネットを開けて配線を変える等によってエンジンを始動させるような場合にも、エンジンの始動時に特定通信端末が周囲に存在するかどうかを判別することによって、悪意の第三者による交通機関の盗難等を早期に解決することができる。

【0164】

【発明の効果】以上説明したように請求項1記載の発明によれば、撮像手段および撮像データ記憶手段が備わっているいはその近傍に埋め込まれるので、自分が撮影されたことに気づいた侵入者等は撮影された画像を消去したり撮像データ記憶手段自体を取り出すことが困難であり、早急に現場を立ち去ることになり、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。また銀塩写真と比べてランニングコストをわずかに抑えることができ、また事件が起きたときには画像データを有効な資料とすることができる。

【0165】また請求項2記載の発明によれば、撮像手段のみならず撮像データ発信手段も備わっているいはその近傍に埋め込まれているので、発信を安全に行うことができる。しかも本発明の場合には画像自体は所定の受信先に送られてしまうので、仮に撮像手段や撮像データ発信手段が持ち去られたとしても、画像の記録は残ることになり、結果的に無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【0166】更に請求項3記載の発明によれば、小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮

影することしたので、ドア自体を加工する必要がなく有効なセキュリティシステムを実現することができる。またドアノブを交換する場合もドアを取り替えて改造を行う場合に比べると遙かに安価であり、経済的なシステムを構成することができる。更に、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【0167】また、請求項4記載の発明によれば、小型化された撮像のための装置をドアノブあるいはこのドアノブとドアとの間に配置されたドアノブの台座の孔から撮影することにしたので、ドア自体を加工する必要がなく有効なセキュリティシステムを実現することができる。またドアノブを交換する場合もドアを取り替えて改造を行う場合に比べると遙かに安価であり、経済的なシステムを構成することができる。しかも撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信する。したがって、事故の発生や火事等の来訪を迅速に知ることができる。更に、台座の表面に凹凸を付けるといったようにデザインを工夫すれば、孔の存在を判りにくくすることができる。

【0168】更に請求項5記載の発明によれば、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿つので、ドア自体を加工する必要がない。したがって、現在使用している交通機関を簡単に改造することができ、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【0169】また請求項6記載の発明によれば、自動車、船等の交通機関のドアの外側部分に突出して取り付けられたドアの把手あるいはこの把手に取り付けられた付属部品に孔を穿つので、ドア自体を加工する必要がない。したがって、現在使用している交通機関を簡単に改造することができ、無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。しかも撮像データ発信手段は、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するので、その交通機関自体が盗難にあった場合でも撮像データ自体は安全な箇所に保持されることになり、盗難等に関係した者の特定が容易になる。

【0170】更に請求項7記載の発明によれば、交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容することで、本発明による盗難防止等の利益を得ることができる。

【0171】また請求項8記載の発明によれば、交通機関の外側に予め荷物を止めるための部品やバックミラー等の部品が配置されている場合には、これらの部品の内部に撮像手段等を収容することで、本発明による盗難防止等の利益を得ることができる。しかも本発明では撮像

データ発信手段を配置しているので、撮像データ自体は安全な場所に送信され、かつ画像データを早期に取得できることになる。

【0172】更に請求項9記載の発明によれば、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっているので、特別の通路や部屋を有効に監視することができる。

【0173】また請求項10記載の発明によれば、撮像手段が通路または部屋の壁に埋め込まれ壁の前の被写体を撮像することができるようになっているので、特別の通路や部屋を有効に監視することができる。しかも本発明では撮像データ発信手段を配置しているので、撮像データ自体は安全な場所に送信され、かつ画像データを早期に取得できる。

【0174】更に請求項11記載の発明によれば、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしたので、借家主まいのように扉または通路自体の改造が難しい場合にも、このような容器を適所に取り付けすることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。

【0175】また請求項12記載の発明によれば、郵便受けやドアホン等のように人の出入りする扉または通路の周辺に配置された防犯以外の所定の用途に使用される容器に孔を穿ち、撮像手段でこの孔を通して外部を撮影するようにしたので、借家主まいのように扉または通路自体の改造が難しい場合にも、このような容器を適所に取り付けすることで、泥棒等の無断侵入や盗難あるいは不正行為の発生を有効に防止することができる。しかも撮像データ発信手段が、トリガ手段によって作動した撮像手段から得られる撮像データを所定の受信先に発信するようになっている。したがって、その容器自体を破壊されたり持ち去られるような場合でも、その行為を行った者の画像を取得することができ、結果的にそのような行為自体も防止することができる。

【0176】更に請求項13および請求項14記載の発明によれば、所定のタイミングを検出して撮像を行うこととしたので、撮像されたデータが有効なものが多く、かつ画像データの記憶容量が少なくて良いという利点がある。

【0177】また、請求項15記載の発明によれば、トリガ手段は、予め定めた時間ごとに撮像手段を作動させるので、トリガ用に特別のセンサが不要である。また、人の検出を行う必要がないので、撮影の隙間が適正であれば確実に無断侵入や盗難あるいは不正行為に関する画像を記録することができるという長所がある。

【0178】更に請求項16記載の発明によれば、撮像手段の近傍に外部の音を収集するマイクが配置されているので、採取するデータが豊富化される。

【0179】また請求項17記載の発明によれば、孔はキーホールに似せた撮像のための孔であるので、ドア等の外観を損ねる可能性が小さい。

【0180】更に請求項18記載の発明では、撮像の時刻情報が撮像データに組み込まれるので、泥棒等の無断侵入や盗難あるいは不正行為の起きた日時を推測できるだけでなく、たとえば子供が学校から帰ってきた時間等も簡単に知ることができる。

【0181】また請求項19記載の発明によれば、記憶手段に静止面の画像データを1枚ずつ記憶する場合に、ある程度のメモリ容量に対して古い画像から順に上書きして記憶することで、メモリ不足を解消することができ、特別の事件が起きた時点で画像データを確実に再現することができる。

【0182】更に請求項20記載の発明によれば、携帯端末を受信先とすることで迅速な対応が可能になる。また撮像側に音声の入出力装置を備えることで、訪問者との会話が可能になる。

【0183】また請求項21記載の発明によれば、所定の発信先が駐輪場あるいは駐車場等に設けられた集中管理用の通信端末なので、それぞれの発信元ごとにデータが管理されれば、安面に盗難やいたずらの防止が可能になる。

【0184】更に請求項22記載の発明によれば、撮像データを屏の配置されている側から所定の発信先へ発信し、この通信中に発信先から開錠を指示する信号が送られてきたとき扉を開錠するので、屏の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の速否を的確に判断することができる。しかも、第三者の発呼によって開錠すると異なるので、セキュリティを高度に保持することができる。

【0185】また請求項23記載の発明によれば、撮像データ発信手段の発信先に撮像データを発信できないとき、予め定めた宛先にこれを転送し、その転送先がこれによる通信を行っている場合に限り遠隔操作による開錠を可能にしたので、本来の発信先の都合によって扉を開けるまでの待ち時間が長くなったたり不可能となるといった事態が発生しない。また、本発明の場合にも屏の前の被写体を撮像データで確認したり音声による確認が可能であり、開錠の速否を的確に判断することができる。しかも、第三者の発呼によって開錠すると異なるので、セキュリティを高度に保持することができる。

【0186】更に請求項24記載の発明によれば、孔から撮像手段が撮像する障害となる明るさの変化を検出する障害検出手段と、この障害検出手段の検出が行われたとき警報音を出力する警報音出力手段を具備しているので、犯罪の予備行為が行われていることを第三者に知らせ、犯罪の発生を防止することができる。

【0187】また請求項25記載の発明によれば、孔から撮像手段が撮像する障害となる明るさの変化を検出す

る障害検出手段と、この障害検出手段の検出が行われたとき警報を示すデータを所定の宛先に送出する警報データ送出手段を具備しているため、犯罪の予備行為が行われていることを関係者に知らせ、必要な措置を採ることができる。

【0188】更に請求項26記載の発明では、撮影を行うための孔を複数配置し、障害検出手段が1つの孔の障害を検出したとき他の孔の内部に配置された撮像手段を作動させることにしたので、撮影の妨害を行う者が1つの孔を塞ぐ等の行為を行っても、他の孔を通じて画像を取得することができ、セキュリティを向上させることができる。

【0189】また請求項27または請求項28記載の発明によれば、交通機関を走行させる者の多くが自己の通信のための携帯電話機等の通信端末を所持している事実を鑑みて、動力源始動検出手段が何らかの操作で動力源の始動を検出したときその周囲にその者の通信端末（特定通信端末）が存在していないときにはその特定通信端末に無線で通知することで、第三者による交通機関の無断走行等に対処することができる。

【0190】特に請求項28記載の発明では、自動車の運転者がキーをキー挿入口に差したままにしているような場合であっても、これによる盗難事件を早期に解決することができる。また、特定通信端末とその交通機関との間で音声等の通信を行うことも簡単に可能になる。

【0191】更に請求項29記載の発明によれば、たとえばキー挿入口の近傍等の第三者が気づきにくい位置等に撮像手段を配置しておけば、これらの者が不正に運転を試みた場合にその者の画像を特定通信端末に送信することが可能になる。また、交通機関の所有者の家族がその交通機関を運転しようとしたような場合には、画像を見ることによって第三者が不正に操作しているものでないことを簡単に確認することができる。

【0192】また請求項30記載の発明によれば、交通機関側制御手段は、通知手段の通知に基づいて前記した特定通信端末から交通機関の走行停止あるいはドアのロックを示す信号が送信されてきたときこれに応じてその交通機関の走行停止あるいはドアのロックを行うので、交通機関が行方をくらましたり不正に運転を行った者が運転席から速やかなる事態の発生を防止することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例におけるセキュリティシステムの構成の概要を表わした正面図である。

【図2】第1の実施例で使用されるセキュリティシステムの要部を示す断面図である。

【図3】第1の実施例の変形例としてのセキュリティシステムを屋内から見た要部斜視図である。

【図4】本発明の第2の実施例におけるセキュリティシステムの構成の概要を表わした正面図である。

【図5】第2の実施例における郵便ポストの構成を示した説明図である。

【図6】本発明の第3の実施例におけるセキュリティシステムが適用される金庫の斜視図である。

【図7】第3の実施例の第1の変形例として公衆トイレの防犯用のセキュリティシステムを表わした正面図である。

【図8】第3の実施例の第2の変形例としてエレベータの防犯用のセキュリティシステムを表わした正面図である。

【図9】本発明の第4の実施例におけるドアノブを使用したセキュリティシステムの要部を表わした平面図である。

【図10】第4の実施例の変形例としてセキュリティシステムを使用した自動車の側面図である。

【図11】本発明の第5の実施例のセキュリティシステムの概要を表わしたシステム構成図である。

【図12】本発明の第6の実施例のセキュリティシステムの概要を表わしたシステム構成図である。

【図13】本発明の第7の実施例のセキュリティシステムの概要を表わした正面図である。

【図14】本発明の第7の実施例におけるドアの要部の断面構造を表わした断面図である。

【図15】本発明の第7の実施例における電子式錠装置の開錠制御の様子を表わした流れ図である。

【図16】本発明の第7の実施例における悪意の来訪者が撮影を妨害する場合の対策としての処理の流れを表わした流れ図である。

【図17】本発明の第8の実施例のセキュリティシステムの要部を表わした概略構成図である。

【図18】第8の実施例の無線送受信器付制御装置の制御の概要を表わした流れ図である。

【図19】本発明の第9の実施例のセキュリティシステムの概要を表わしたシステム構成図である。

【図20】第9の実施例における装置内通信端末の制御の様子を表わした流れ図である。

【図21】第9の実施例のセキュリティシステムの变形例としての特定携帯電話機のセキュリティシステムの要部を表わした説明図である。

【図22】この变形例における装置内通信端末側の処理の流れを示した流れ図である。

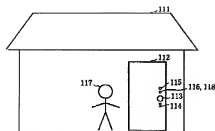
【図23】本発明の第10の実施例のセキュリティシステムの要部を表わしたドアの正面図である。

【符号の説明】

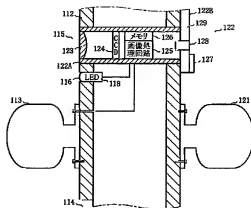
- 111 家屋
- 112、282、283 ドア
- 113、253 ドアノブ
- 114 キーホール

- 118 赤外線LED（発光ダイオード）ランプ
- 122 画像ユニット
- 124 CCD
- 126 メモリ
- 127 スイッチ
- 128、261 画像データ出力端子
- 129 液晶ディスプレイ
- 144、305、325 受信装置
- 161 郵便ポスト
- 166～168、183、184、206～209、232、233、258、259、504 孔
- 171、186 画像処理ユニット
- 173、185 送信アンテナ
- 181 金庫
- 182 扉
- 201 公衆トイレ
- 231 エレベータ
- 251、252 ノブ
- 257 画像撮影処理ユニット
- 281、302 自動車
- 284、285 ドアの把手
- 286、287 付属装置
- 301 自転車
- 303 バイク
- 304 駐車場
- 321、322 絵画
- 324 撮像送信ユニット
- 401 電子式錠装置
- 402 セキュリティ装置
- 411、413 基地局
- 414 セキュリティ管理会社
- 415 携帯電話端末
- 421 スピーカ部
- 422 マイク部
- 423 制御部
- 425 無線アンテナ
- 501 ボード
- 502 キー挿入口
- 503 孔の集合体
- 505 撮像装置
- 506 スピーカ
- 507 マイクロフォン
- 508 エンジン始動検出回路
- 511、511A 装置内通信端末
- 512、512A 携帯電話機
- 551 近距離通信カード
- 592 撮像用孔

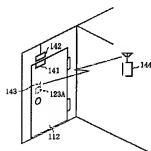
【図1】



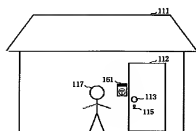
【図2】



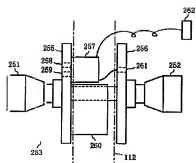
【図3】



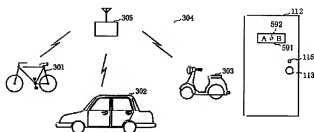
【図4】



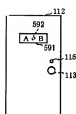
【图9】



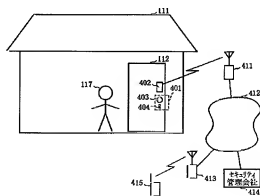
【图 1-1】



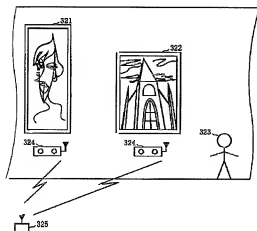
【图23】



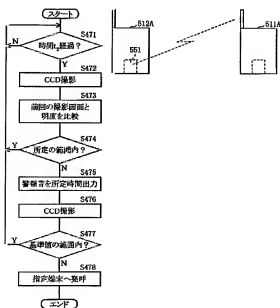
【例13】



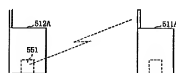
【图 12】



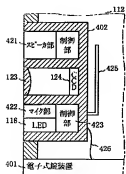
【图16】



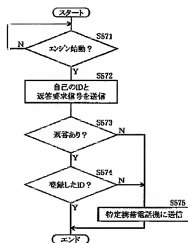
【图21】



【图 14】



【図22】



フロントページの続き

(51)Int. Cl. ⁷	識別記号	F I	(参考)
G 0 8 B 21/00		G 0 8 B 21/00	E
H 0 4 N 5/225		H 0 4 N 5/225	C
7/18		7/18	D
			H
// H 0 4 N 101:00		101:00	

(72)発明者 山口 寛一
東京都新宿区西新宿5-17-11

Fターム(参考) 2E250 A421 B808 B815 B865 C000
CC21 CC28 D006 FF24 FF25
FF27 FF36 HH00 HH01 JJ00
KK03 LL00 LL01 PP15 SS04
TT03
5C022 AA01 AA13 AC42
5C054 AA01 AA05 BA10 CC05 CE06
CH04 DA07 HA18
5C084 AA02 AA07 BB31 CC02 CC19
DD11
5C086 AA27 BA02 BA21 CA28 CB36
DA08 DA33 FA02